

# PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA W NOWYM SĄCZU

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2013/2014

Instytut Techniczny

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: Niestacjonarne

Kod kierunku: 11.3

Stopień studiów: I

Specjalności: Informatyka stosowana

### 1 PRZEDMIOT

NAZWA PRZEDMIOTU	Bezpieczeństwo technologii informatycznych
KOD PRZEDMIOTU	IT 11.3 AIN C9 13/14
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	3
SEMESTRY	6

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	PROJEKT	SEMINARIUM
6	8			15	

### 3 CELE PRZEDMIOTU

**Cel 1** Zapoznanie studenta z podstawami zabezpieczenia technologii informatycznych i sieciowymi protokołami zabezpieczającymi.

**Cel 2** Nabycie przez studenta wiedzy o metodach kryptoanalitycznych.

**Cel 3** Wykształcenie umiejętności określenia przydatności algorytmów kryptograficznych z kluczem publicznym i symetrycznych, oraz wybierania i stosowania właściwych trybów działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.

**Cel 4** Wykształcenie umiejętności oceny przydatności i sposobu działania, istniejących rozwiązań zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.

**Cel 5** Wykształcenie umiejętności projektowania prostych układów i aplikacji w zakresie systemów kryptograficznych oraz ich konfigurowania i administrowania.



## 4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- a Matematyka dyskretna.
- b Metody probabilistyczne i statystyka.
- c Podstawy elektroniki i miernictwa.
- d Języki i paradygmaty programowania.
- e Technologia sieciowa.

## 5 EFEKTY KSZTAŁCENIA

**EK1** Wiedza: Student zna i opisuje podstawy zabezpieczenia technologii informatycznych i sieciowe protokoły zabezpieczające.

**EK2** Wiedza: Student objaśnia metody kryptoanalityczne.

**EK3** Umiejętności: Student potrafi określić przydatność i użyć algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz dobrać właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.

**EK4** Umiejętności: Student ocenia przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.

**EK5** Kompetencje społeczne: Student potrafi określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.

## 6 TREŚCI PROGRAMOWE

### WYKŁAD

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BŁOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Podstawy bezpieczeństwa technologii informatycznych. Kryptograficzne systemy zabezpieczenia technologii informatycznych.	1
W2	Algorytm RSA oraz inne algorytmy z kluczem publicznym. Sposoby generowania i zastosowania sekwencji pseudolosowych.	1
W3	Kryptograficzne algorytmy symetryczne DES, TDES, Twofish, Blowfish, CAST, GOST, IDEA, RC5, AES.	1
W4	Tryby działań algorytmów symetrycznych.	1
W5	Administracja kluczami i protokoły uzgadniania kluczy. Sieciowe protokoły zabezpieczające.	1
W6	Zabezpieczenia dostępu do informacji. Karty elektroniczne. Systemy steganograficzne.	1
W7	Zabezpieczające metody biometryczne. Poziomy bezpieczeństwa systemów kryptograficznych.	1
W8	Techniki i metody kryptoanalityczne.	1
	RAZEM	8



## PROJEKT

LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P1	Zarządzanie i konfigurowanie dostępu lokalnego do systemu Windows, konfigurowanie mechanizmów podnoszących bezpieczeństwo systemu.	1
P2	Zarządzanie i konfigurowanie dostępu lokalnego do systemu Linux, konfigurowanie mechanizmów podnoszących bezpieczeństwo systemu.	1
P3	Metody zarządzania bezpieczeństwem serwerowych systemów operacyjnych Linux.	1
P4	Metody zarządzania bezpieczeństwem serwerowych systemów operacyjnych Windows.	1
P5	Stosowanie metod kryptograficznych do ochrony przesyłanych informacji w warstwie aplikacji.	1
P6	Stosowanie bezpiecznych protokołów sieciowych. Tworzenie sieci VPN.	1
P7	Budowa i konfiguracja zapory sieciowej (firewall).	1
P8	Integracja mechanizmów kryptograficznych z usługami pocztowymi.	1
P9	Metody wykrywania intruzów w sieciach komputerowych.	2
P10	Budowa i konfiguracja zabezpieczeń usług aplikacyjnych (np. www).	1
P11	Testy penetracyjne - techniki skanowania, sniffing, spoofing, ataki odmowy usługi (Denial of Service).	2
P12	Ograniczenie środowiska wykonywania aplikacji, powłoki środowisk serwerowych, delegacja uprawnień administracyjnych.	1
P13	Procedury tworzenia polityki bezpieczeństwa.	1
	RAZEM	15

## 7 METODY DYDAKTYCZNE

M1 Wykłady

M2 Prezentacje multimedialne

M3 Ćwiczenia projektowe

## 8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
<b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>	
Godziny wynikające z planu studiów	23
Konsultacje przedmiotowe	1
Egzaminy i zaliczenia w sesji	0
<b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b>	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	31
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	20
<b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA</b>	<b>75</b>
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3



## 9 SPOSOBY OCENY

### OCENA FORMUJĄCA

**F1** Odpowiedź ustna

**F2** Aktywność na zajęciach

**F3** Projekt indywidualny

**F4** Projekt zespołowy

### KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 1
NA OCENĘ 3	Student nazywa i opisuje podstawy zabezpieczenia technologii informatycznych i sieciowe protokoły zabezpieczające, ale z błędami.	wykład, projekt	Ocena z odpowiedzi ustnych, aktywności na zajęciach i ćwiczeń projektowych.
NA OCENĘ 4	Student zna motywacje badań nad zabezpieczeniem technologii informatycznych, interpretuje sieciowe protokoły zabezpieczające, z drobnymi nieścisłościami.		
NA OCENĘ 5	Student ze znawstwem opisuje podstawy zabezpieczenia technologii informatycznych i bezbłędnie prezentuje sieciowe protokoły zabezpieczające.		
EFEKT KSZTAŁCENIA 2		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 2
NA OCENĘ 3	Student nazywa i rozróżnia metody kryptoanalityczne, ale nie potrafi wyjaśnić ich sedna.	wykład, projekt	Ocena z odpowiedzi ustnych, aktywności na zajęciach i ćwiczeń projektowych.
NA OCENĘ 4	Student rozpoznaje, kategoryzuje i ocenia metody kryptoanalityczne, z drobnymi nieścisłościami.		
NA OCENĘ 5	Student ze znawstwem rozpoznaje, kategoryzuje i ocenia metody kryptoanalityczne. Podaje przykłady.		
EFEKT KSZTAŁCENIA 3		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 3
NA OCENĘ 3	Student, popełniając błędy, określa przydatność i używa algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz dobiera właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.	projekt	Ocena z ćwiczeń projektowych.
NA OCENĘ 4	Student określa przydatność i używa algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz dobiera właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych, ale z drobnymi nieścisłościami.		



NA OCENĘ 5	Student prawidłowo określa przydatność i używa algorytmy kryptograficzne z kluczem publicznym i symetryczne, oraz bezbłędnie dobiera właściwy tryb działań algorytmów symetrycznych do rozwiązywania prostych zadań bezpieczeństwa technologii informatycznych.		
EFEKT KSZTAŁCENIA 4		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 4
NA OCENĘ 3	Student, popełniając błędy, jest w stanie ocenić przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.	projekt	Ocena z ćwiczeń projektowych.
NA OCENĘ 4	Student ocenia przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych, ale z drobnymi nieścisłościami.		
NA OCENĘ 5	Student ocenia ze znanostwem przydatność i sposób działania, istniejące rozwiązania zabezpieczenia dostępu do informacji, w tym przy pomocy kart elektronicznych i metod biometrycznych.		
EFEKT KSZTAŁCENIA 5		MIEJSCE WERYFIKACJI	OPIS WERYFIKACJI EK 5
NA OCENĘ 3	Student potrafi z trudem i częściowo określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.	projekt	Ocena z ćwiczeń projektowych.
NA OCENĘ 4	Student potrafi niektóre określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.		
NA OCENĘ 5	Student potrafi w pełni określić cele ekonomiczne i podejmować nowe wyzwania projektowe i biznesowe w zakresie inżynierii bezpieczeństwa technologii i systemów informatycznych z uwzględnieniem algorytmów kryptograficznych.		

**OCENA DO INDEKSU (OCENA PODSUMOWUJĄCA)**

Średnia ważona ocen częściowych uzyskanych za poszczególne efekty kształcenia.



## WARUNKI ZALICZENIA PRZEDMIOTU

a Zaliczenie na podstawie obecności i aktywnego udziału w wykładach, oraz wyników oceny ćwiczeń projektowych.

## 10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKTY KSZTAŁCENIA DLA PRZEDMIOTU	ODNIESIENIE DO EFEKTÓW KIERUNKOWYCH	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	METODY DYDAKTYCZNE
EK1	INF_W16	Cel1	W1, W5, P1, P2, P6, P13	M1, M2, M3
EK2	INF_W16	Cel2	W8, P11	M1, M2, M3
EK3	INF_UB06	Cel3	W2, W3, W4, P5, P8	M1, M2, M3
EK4	INF_UB01	Cel4	W6, W7, P3, P4, P7, P9, P10, P12	M1, M2, M3
EK5	INF_K06	Cel5	W1, W5, W6, W7, P5, P6, P7, P13	M1, M2, M3

## 11 WYKAZ LITERATURY

### LITERATURA PODSTAWOWA:

- [1] Grzywak A. — *Bezpieczeństwo systemów komputerowych*, Gliwice, 2000, Pracownia Komputerowa Jacka Skalmierskiego
- [2] Karpiński M. — *Bezpieczeństwo informacji*, Warszawa, 2012, PAK
- [3] Majwald E. — *Bezpieczeństwo w sieci kurs podstawowy*, Kraków, 2001, Edition
- [4] Schneider B. — *Kryptografia dla praktyków. Wyd. 2 zm. i rozsz.*, Warszawa, 2002, WNT
- [5] Strebe B. — *Bezpieczeństwo sieci*, Warszawa, 2005, MIKOM

### LITERATURA UZUPEŁNIAJĄCA:

- [1] Wobst R. — *Budowa i łamanie zabezpieczeń*, Warszawa, 2002, READ ME
- [2] x — *Bezpieczeństwo systemów komputerowych*, Warszawa, 2012, <http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%9Bstwo>
- [3] Karpiński M., Kurytnik I.P. — *Sieci komputerowe: Bezpieczeństwo. Część 1 Metody i systemy kryptograficzne*, Bielsko-Biała, 2006, ATH

## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

prof. dr hab. inż. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

### OSOBY PROWADZĄCE PRZEDMIOT

prof. dr hab. inż. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

mgr Grzegorz Litawa (kontakt: glitawa@poczta.onet.pl)



## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(kierownik zakładu)

(dyrektor instytutu)

PWSZ w Nowym Sączu

**PRZYJMUJĘ DO REALIZACJI** (data i podpisy osób prowadzących przedmiot)

.....

.....